(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 658 054 A2**

(12) EUROPEAN PATENT APPLICATION

(21) Application number: **94119403.7**

(51) Int. Cl.[6]: **H04N 7/16**, H04N 7/167

(22) Date of filing: **08.12.94**

(30) Priority: **09.12.93 IL 10796793**

(43) Date of publication of application: **14.06.95 Bulletin 95/24**

(84) Designated Contracting States: **AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL PT SE**

(71) Applicant: **NEWS DATACOM LTD.**
POB 495,
Virginia Street
London E1 9XY (GB)

(72) Inventor: **Nachman, Jacob Bezalel**
3 Hatamar Street
Ramat Modiim 73127 (IL)
Inventor: **Tsuria, Yossef**
20 Shalom Sivan Street
Jerusalem 97276 (IL)

(74) Representative: **Modiano, Guido, Dr.-Ing. et al**
Modiano, Josif, Pisanty & Staub,
Baaderstrasse 3
D-80469 München (DE)

(54) Apparatus and method for securing communication systems.

(57) A hacking prevention system for use with a network including a transmitter and a multiplicity of receivers, each receiver being independently enabled by a secret number and when enabled being responsive to data received from the transmitter for decrypting encrypted information, each of the multiplicity of receivers including: a first key generator, employing at least part of the data and a function which differs for at least a plurality of ones of the multiplicity of receivers, for generating a first key which is different for each receiver having a different function, a second key generator employing at least part of the data and the function to produce a second key, and a secret number generator utilizing the first key with the second key to produce the secret number which is the same for all of the multiplicity of receivers, whereby first and second keys intercepted at a first receiver cannot be effective to enable a second receiver having a different function.

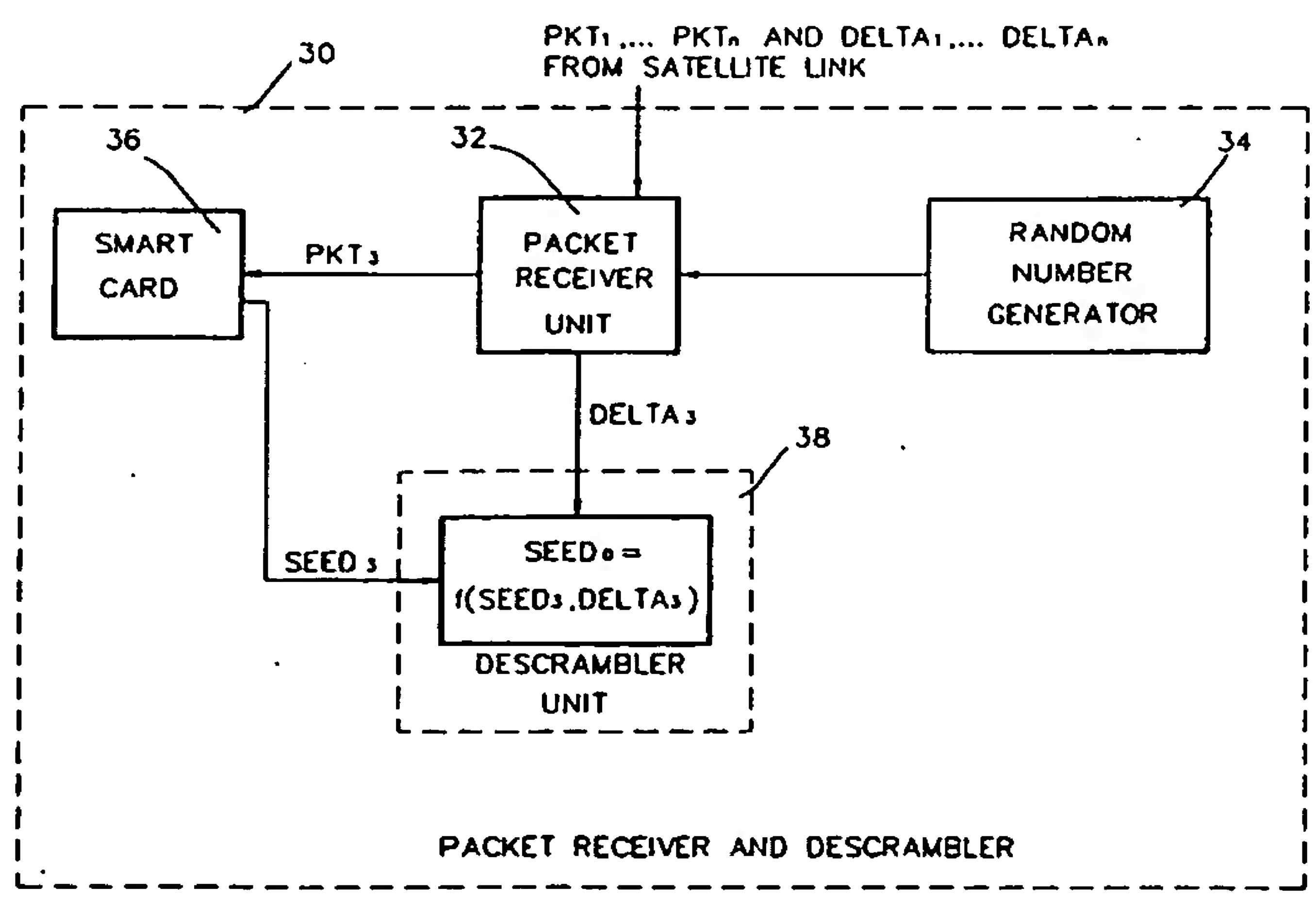

FIG. 2

Rank Xerox (UK) Business Services

FIELD OF THE INVENTION

The present invention relates generally to secure communication systems and more particularly to systems wherein encrypted information is transmitted from a single location to multiple terminals located at non-secure locations.

BACKGROUND OF THE INVENTION

A major problem in secure communication systems is the possibility of unauthorized penetration. Unauthorized penetration of this kind is referred to as hacking.

Several methods have been employed to overcome the problem of hacking. Encryption of transmitted data and authentication of communicators are some of the methods employed to make hacking more difficult.

One hacking method which is considered difficult to overcome is called "The McCormac Hack". This method, which is believed to be theoretically applicable to CATV systems, is described in the book "World Satellite TV and Scrambling Methods", 2nd Edition, Baylin Publications 1991, pp. 243 - 244 by Frank Baylin, Richard Maddox and John McCormac and in "Satellite Watch News", August 1991. According to this method, a data stream from a legitimately authorized decoder, is extracted in real time and transmitted over the air using a small radio-frequency (RF) transmitter. The data stream is then used to activate a number of pirate decoders.

SUMMARY OF THE INVENTION

The present invention seeks to provide methods and systems which substantially prevent the possibility of extracting a data stream from a legitimately authorized terminal and transmitting the data stream to a plurality of pirate terminals.

For the purposes of the present invention, the term "terminals" in all of its forms is used in a broader than usual sense to cover all types of computer terminals, CATV decoders, remote computers and remote computerized stations.

For the purposes of the present invention, the terms "seed" and "key" in all of their forms are alternately used in a broader than usual sense to cover all types of numbers or other symbols, either secret or non-secret, which are used at least as part of encryption/decryption keys to encrypt/decrypt (or scramble/descramble) data. The term "secret number" will be further used, for the purpose of the present invention, to denote the secret key which is used for encryption/decryption (or scrambling/descrambling) of data.

There is thus provided in accordance with a preferred embodiment of the present invention a hacking prevention system for use with a system including a transmitter and a multiplicity of receivers, each receiver being independently enabled by a secret number and when enabled being responsive to data received from the transmitter for decrypting encrypted information, each of the multiplicity of receivers having associated therewith:

a first key generator, employing at least part of the data and a function which differs for at least a plurality of ones of said multiplicity of receivers, for generating a first key which is different for each receiver having a different function;

a second key generator employing at least part of the data and said function to produce a second key; and

a secret number generator utilizing the first key with the second key to produce said secret number which is the same for all of said multiplicity of receivers,

whereby first and second keys intercepted at a first receiver cannot be effective to enable a second receiver having a different function.

Additionally in accordance with a preferred embodiment of the present invention there is provided a hacking prevention method for use with a network including a transmitter and a multiplicity of receivers, each receiver being independently enabled by a secret number and when enabled being responsive to data received from the transmitter for decrypting encrypted information, the method comprising the steps of:

generating a first key, by employing at least part of the data and a function which differs for at least a plurality of ones of the multiplicity of receivers, the first key being different for each receiver having a different function;

generating a second key by employing at least part of the data and the function; and

generating a secret number by utilizing the first key with the second key to produce the secret number which is the same for all of the multiplicity of receivers,

whereby first and second keys intercepted at a first receiver cannot be effective to enable a second receiver having a different function.

Additionally in accordance with a preferred embodiment of the present invention there is provided a system for selective transmission of information to a multiplicity of subscribers which subscribers may be individually characterized by at least one of the following parameters: information suppliers, geographic locations, and demographics, wherein information is transmitted from an information source to a multiplicity of subscribers which fall into different groups according to at least one of the parameters, each group being entitled to re-

ceive at least a portion of the information, the system being employed in a network including a transmitter and a multiplicity of receivers, each receiver associated with a subscriber and being independently enabled by a secret number and when enabled being responsive to data received from the transmitter for decrypting encrypted information, each of the multiplicity of receivers comprising:

a first key generator, employing at least part of the data and a function which differs for at least a plurality of ones of the multiplicity of receivers, for generating a first key which is different for each receiver having a different function;

a second key generator employing at least part of the data and the function to produce a second key;

a third key generator employing at least part of the data to provide a key which is characterized by at least one of the parameters; and

a secret number generator utilizing the first key, the second key and the third key to produce the secret number which is the same for all of the multiplicity of receivers,

whereby first and second keys intercepted at a first receiver cannot be effective to enable a second receiver having a different function, and

whereby a third key intercepted at a receiver which forms part of a first group of receivers cannot be effective to enable a receiver which forms part of a second of the group of receivers.

Further in accordance with a preferred embodiment of the present invention there is provided a method for selective transmission of information to a multiplicity of subscribers which subscribers may be individually characterized by at least one of the following parameters: information suppliers, geographic locations, and demographics, wherein information is transmitted from an information source to a multiplicity of subscribers which fall into different groups according to at least one of the parameters, each group being entitled to receive at least a portion of the information, the method being employed in a network including a transmitter and a multiplicity of receivers, each receiver associated with a subscriber and being independently enabled by a secret number and when enabled being responsive to data received from the transmitter for decrypting encrypted information, the method comprising the steps of:

generating a first key by employing at least part of the data and a function which differs for at least a plurality of ones of the multiplicity of receivers, for generating a first key which is different for each receiver having a different function;

generating a second key by employing at least part of the data and the function to produce a second key;

generating a third key by employing at least part of the data to provide a key which is characterized by at least one of the parameters; and

generating a secret number utilizing the first key, the second key and the third key to produce the secret number which is the same for all of the multiplicity of receivers,

whereby first and second keys intercepted at a first receiver cannot be effective to enable a second receiver having a different function, and

whereby a third key intercepted at a receiver which forms part of a first group of receivers cannot be effective to enable a receiver which forms part of a second of the group of receivers.

In accordance with a preferred embodiment of the present invention, the function which differs for at least a plurality of ones of said multiplicity of receivers, is a random generator.

Preferably, the second key generator is embodied in a single VLSI chip.

In accordance with a preferred embodiment of the present invention, the VLSI chip is mounted on a smart card.

Preferably, the first key generator, the function and the secret number generator are embodied in a single VLSI chip.

In accordance with a preferred embodiment of the present invention, the first key generator, the function, the secret number generator and the second key generator are embodied in a single VLSI chip.

Preferably, each of said multiplicity of receivers comprises at least one of said VLSI chips.

In accordance with a preferred embodiment of the invention, the network is a CATV network and said multiplicity of receivers are CATV receivers and decoders.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated more fully from the following detailed description, taken in conjunction with the drawings in which:

Fig. 1 is a generalized block diagram illustration of a theoretical hacking system based on the prior art "McCormac Hack" method;

Fig. 2 is a generalized block diagram illustration of part of a subscriber unit constructed and operative in accordance with a preferred embodiment of the present invention;

Fig. 3 is a flowchart description of the functionality of the apparatus of Fig. 2;

Fig. 4 is a flowchart description of the functionality of the apparatus of Fig. 2 in accordance with an alternative embodiment of the invention which does not employ conditional access cards;

Fig. 5 is a generalized block diagram illustration of part of a subscriber unit in accordance with a preferred embodiment of the invention in which receivers characterized by different parameters are enabled with the same secret number; and

Fig. 6 is a flowchart description of the functionality of the apparatus of Fig. 5.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Reference is now made to Fig. 1, which is a generalized block diagram illustration of a theoretical hacking system constructed and operative in accordance with the prior art "McCormac Hack" method.

An authorized decoder 10, which is normally operated by a valid smart card 12, is coupled instead to a McCormac's Hack Interface (MHI) unit 14 via a standard smart card communication link 15. Smart card 12 is also coupled to the MHI unit 14 via a standard smart card communication link 16.

MHI unit 14 "sniffs" the communication data passed between the smart card 12 and the authorized decoder 10 and provides it to a small radio transmitter 18. Radio transmitter 18 transmits the data via a radio-frequency (RF) link 19 to a radio receiver 20 which is coupled to a virtual smart card unit 22. Virtual smart card unit 22 is coupled to an unauthorized decoder 24 via a standard smart card communication link 25. In this way the unauthorized decoder 24 is operated by the same data stream that operates the authorized decoder 10.

In an alternative embodiment, MHI unit 14 "sniffs" the data which is communicated between units inside the authorized decoder 10. In this embodiment, MHI unit 14 is linked, via communication link 27, to a communication BUS 26 extending between a micro-processor 28 and a descrambling device 29. Communication BUS 26 carries the "seed" value which is the secret number required for descrambling. In this way the seed value may be extracted and transmitted to the unauthorized decoder for descrambling of the data.

Reference is now made to Fig. 2, which is a generalized block diagram illustration of part of a subscriber unit constructed and operative in accordance with a preferred embodiment of the present invention.

In accordance with a preferred embodiment of the present invention, a data stream including a series of authorization packets PKT1,...,PKTn is transmitted from an information source via a satellite link, to a packet receiver and descrambler unit 30 which forms part of a subscriber's CATV receiver and decoder (not shown). A series of offset values DELTA1,...,DELTAn is also transmitted via the satellite link and received by the packet receiver and descrambler unit 30. Preferably, each packet is paired with an offset value.

In the packet receiver and descrambler unit 30 a Packet Receiver Unit (PRU) 32 receives the series of packets and the offset values. A random number generator 34 provides a number in the range 1,...,n to PRU 32 by employing a random number algorithm. According to the selected number, for example 3, the corresponding packet, i.e. PKT3, is transmitted to a smart card 36 and a corresponding offset value, i.e. DELTA3, which serves as an internal key, is transmitted to a descrambler unit 38.

Smart card 36 employs an algorithm which produces an appropriate seed for each packet. When smart card 36 receives PKT3 it produces a corresponding key, here termed SEED3, and provides it to the descrambler unit 38.

It is to be appreciated that PRU 32, random number generator 34 and the descrambler unit 38 are all embodied in a secure chip such as a VLSI chip. Thus, the communication of the random number and the offset value cannot be altered or "sniffed".

In the descrambler unit 38 the keys DELTA3 and SEED3 received from PRU 32 and smart card 36 respectively are employed by a function f such that:

(1) f = f(seed value, offset value), and

(2) SEED0 = f(SEEDi,DELTAi) for any i = 1,...,n, where SEED0 is the secret number required for descrambling of the data and "i" is any integer value in the series 1,...,n. If the value i = 3 is selected then:

(3) SEED0 = f(SEED3,DELTA3).

In accordance with a preferred embodiment of the present invention, the descrambler 38 functions as a secret number generator in generating the SEED0 value and also functions as a key receiver, which receives an internal key and a key from the smart card. The SEED0 value is employed by the descrambler 38 for descrambling of the data. Inasmuch as the descrambler 38 is in a VLSI format it is considered difficult, if not practically impossible, to tap the SEED0 value.

It is to be appreciated that the hacking prevention system of Fig. 2 may be also operable with systems which do not employ smart cards. In that case the seed values corresponding to the packets PKT1,...,PKTn may be calculated and produced in any suitable part of the packet receiver and descrambler 30, such as, for example, any one of PRU 32, random number generator 34 and descrambler 38, by employing an algorithm which is similar to the one employed in the smart card. Upon receipt of the selected random number from

random number generator 34, the corresponding calculated seed value and the appropriate offset value are provided to descrambler unit 38.

Reference is now made to Fig. 3 which is a flowchart description of the functionality of the apparatus of Fig. 2.

A series of data packets PKT1,...,PKTn and a series of offset values DELTA1,...,DELTAn are received via a satellite link. A random number generation algorithm is employed to calculate and select one of the index numbers 1,...,n. The output of the random number generation algorithm is, for example the index 3. The packet whose index number was calculated, i.e. PKT3, is transmitted to the smart card. In the smart card an algorithm which calculates seeds is employed to calculate the corresponding SEED3 number. SEED3 is then transmitted to descrambler unit 38.

The offset value which corresponds to the calculated index number, i.e. DELTA3, is transmitted to the descrambling unit 38 where it is combined or otherwise utilized, by use of a secret number generator, with SEED3, to calculate a SEED0 value which is the secret number employed to descramble the satellite transmissions.

Reference is now made to Fig. 4 which is a flowchart description of the functionality of the apparatus of Fig. 2 according to an alternative embodiment of the invention. The flowchart of Fig. 4 is similar to the one described in Fig. 3 except that the calculation of the seeds is not performed in a smart card but rather in PRU 32 of Fig. 2. It is to be appreciated that the calculation of the seeds is not limited to PRU 32 but may rather be performed in any part of the secure VLSI chip which forms the packet receiver and descrambler unit 30 shown in Fig. 2.

Reference is now made to Fig. 5 which is a generalized block diagram illustration of part of a subscriber unit in accordance with a preferred embodiment of the invention in which receivers of information supplied by different suppliers or receivers which are otherwise distinguished from each other, as by demographics, geographic location or any other parameter, are enabled with the same secret number.

The system of Fig. 5 is similar to the system of Fig. 2 except that additional data is received from an information source via the satellite link and processed in a packet receiver and descrambler unit 130.

PRU 132 receives, via a satellite link, the following data: a series of packets PKT1,...,PKTn; a series of first offset values DELTA1,...,DELTAn to be employed in part of the abovementioned anti-hacking method; and a series of second offset values GAMMA1,..., GAMMAk.

The series of second offset values GAMMA1,...,GAMMAk is employed to distinguish between separate groups of subscribers/receivers which may be distinguished from each other on the basis of one or more criteria, such as their program suppliers, their geographic location or their demographics. Thus, each group of receivers is characterized by one of the second offset values.

Characterization of the group of receivers can be achieved either by an internal code or an internal algorithm which is entered during manufacture of each decoder, preferably in packet receiver and descrambler 130, or by an algorithm in the smart card which upon its first communication with the decoder causes the decoder to be valid for a selected parameter or group of parameters, as exemplified above. Thus, upon such characterization, each decoder is enabled to select only one of the second offset values GAMMA1,...,GAMMAk.

Alternatively or additionally the characterization of the decoder may be achieved using only the first offset values. In such a case, different decoders may be set to receive only certain ones of the offset values and not others. In this way, the use of the second offset values may be obviated.

If, for example, the decoder is characterized to select GAMMA2, which defines a unique program supplier, PRU 132 will transmit GAMMA2 to descrambler unit 138. Upon selection of a random number, for example 3, by random number generator 134, PRU 132 transmits the respective data packet PKT3 to smart card 136. PRU 132 also transmits an offset value from the series of offset values DELTA1,...,DELTAn according to the selected random number, i.e. DELTA3, to descrambler unit 138.

When issued, the set of smart cards for the subscribers for each group are different from the set of smart cards issued for the subscribers of another group. Differentiation is achieved by employing different algorithms in each set of smart cards. Therefore, for example, even if in two decoders, which are operated by two different information suppliers, the same random number is selected, i.e. 3, and the same data packet is transmitted to both smart cards, i.e. PKT3, each smart card calculates a different seed value, i.e. SEED3 and SEED3'.

Since each of the abovementioned two decoders is operated by a separate program supplier, different second offset values area transmitted to descrambler unit 138, for example GAMMA2 and GAMMA3 respectively.

In the descrambler units 138 of the two decoders the same secret number generator is operated such that:

(4) f = f(seed value, first offset value, second offset value);

(5) SEED0 = f(SEED3, DELTA3, GAMMA2); and also

(6) SEED0 = f(SEED3*, DELTA3, GAMMA3).

It is to be appreciated that in accordance with the abovementioned method the same SEED0 may be employed for descrambling of information originated from one source and targeted to separate groups of subscribers while preventing subscribers of one group from receiving intelligible information destined for another group.

Reference is now made to Fig. 6 which is a flowchart description of the functionality of the apparatus of Fig. 5.

A series of data packets PKT1,...,PKTn, a series of first offset values DELTA1,...,DELTAn and a series of second offset values GAMMA1,...,GAMMAk are received via a satellite link. A random number generation algorithm is employed to calculate and select one of the index numbers 1,...,n. The output of the random number generation algorithm is, for example the index 3. The packet whose index number was calculated, i.e. PKT3, is transmitted to the smart card.

In the smart card an algorithm which calculates seeds is employed to calculate the corresponding SEED3* number. SEED3* is then transmitted to descrambler unit 138.

The first offset value which corresponds to the calculated index number, i.e. DELTA3, is transmitted to the descrambling unit 138. A second offset value which identifies a supplier or jurisdiction, for example GAMMA2, is also transmitted to descrambler unit 138.

In the descrambler unit 138 SEED3*, DELTA3 and GAMMA2 are combined, by use of a secret number generation algorithm, to calculate a SEED0 value which is the secret number employed to descramble the satellite transmissions.

It will be appreciated by persons skilled in the art that the present invention is not limited by what has been particularly shown and described hereinabove. Rather the scope of the present invention is defined only by the claims which follow: Where technical features mentioned in any claim are followed by reference signs, those reference signs have been included for the sole purpose of increasing the intelligibility of the claims and accordingly, such reference signs do not have any limiting effect on the scope of each element identified by way of example by such reference signs.

Claims

1. A hacking prevention system for use with a network including a transmitter and a multiplicity of receivers, each receiver being independently enabled by a secret number and when enabled being responsive to data received from the transmitter for decrypting encrypted information, each of the multiplicity of receivers comprising:

   a first key generator, employing at least part of the data and a function which differs for at least a plurality of ones of the multiplicity of receivers, for generating a first key which is different for each receiver having a different function;

   a second key generator employing at least part of the data and the function to produce a second key; and

   a secret number generator utilizing the first key with the second key to produce the secret number which is the same for all of said multiplicity of receivers,

   whereby first and second keys intercepted at a first receiver cannot be effective to enable a second receiver having a different function.

2. A hacking prevention system according to claim 1 wherein said function which differs for at least a plurality of ones of said multiplicity of receivers, is a random generator.

3. A hacking prevention system according to claim 1 and wherein the second key generator is embodied in a single VLSI chip.

4. A hacking prevention system according to claim 1 wherein the first key generator, the function and the secret number generator are embodied in a single VLSI chip.

5. A hacking prevention system according to claim 1 wherein the first key generator, the function, the secret number generator and the second key generator are embodied in a single VLSI chip.

6. A hacking prevention system according to claim 6 wherein each of said multiplicity of receivers comprises at least one of said VLSI chips.

7. A hacking prevention system according to claim 1 and wherein said network is a CATV network and said multiplicity of receivers are CATV receivers and decoders.

8. A hacking prevention method for use with a network including a transmitter and a multiplicity of receivers, each receiver being independently enabled by a secret number and when enabled being responsive to data received from the transmitter for decrypting encrypted information, the method comprising the steps of:

generating a first key, by employing at least part of the data and a function which differs for at least a plurality of ones of said multiplicity of receivers, said first key being different for each receiver having a different function;

generating a second key by employing at least part of the data and said function; and

generating a secret number by utilizing the first key with the second key to produce said secret number which is the same for all of said multiplicity of receivers,

whereby first and second keys intercepted at a first receiver cannot be effective to enable a second receiver having a different function.

9. A system for selective transmission of information to a multiplicity of subscribers which subscribers may be individually characterized by at least one of the following parameters: information suppliers, geographic locations, and demographics, wherein information is transmitted from an information source to a multiplicity of subscribers which fall into different groups according to at least one of said parameters, each group being entitled to receive at least a portion of the information, the system being employed in a network including a transmitter and a multiplicity of receivers, each receiver associated with a subscriber and being independently enabled by a secret number and when enabled being responsive to data received from the transmitter for decrypting encrypted information, each of the multiplicity of receivers comprising:

a first key generator, employing at least part of the data and a function which differs for at least a plurality of ones of said multiplicity of receivers, for generating a first key which is different for each receiver having a different function;

a second key generator employing at least part of the data and said function to produce a second key;

a third key generator employing at least part of the data to provide a key which is characterized by at least one of said parameters; and

a secret number generator utilizing the first key, the second key and the third key to produce said secret number which is the same for all of said multiplicity of receivers,

whereby first and second keys intercepted at a first receiver cannot be effective to enable a second receiver having a different function, and

whereby a third key intercepted at a receiver which forms part of a first group of receivers cannot be effective to enable a receiver which forms part of a second of said group of receivers.

10. A method for selective transmission of information to a multiplicity of subscribers which subscribers may be individually characterized by at least one of the following parameters: information suppliers, geographic locations, and demographics, wherein information is transmitted from an information source to a multiplicity of subscribers which fall into different groups according to at least one of said parameters, each group being entitled to receive at least a portion of the information, the method being employed in a network including a transmitter and a multiplicity of receivers, each receiver associated with a subscriber and being independently enabled by a secret number and when enabled being responsive to data received from the transmitter for decrypting encrypted information, the method comprising the steps of:

generating a first key by employing at least part of the data and a function which differs for at least a plurality of ones of said multiplicity of receivers, for generating a first key which is different for each receiver having a different function;

generating a second key by employing at least part of the data and said function to produce a second key; .

generating a third key by employing at least part of the data to provide a key which is characterized by at least one of said parameters; and

generating a secret number utilizing the first key, the second key and the third key to produce said secret number which is the same for all of said multiplicity of receivers,

whereby first and second keys intercepted at a first receiver cannot be effective to enable a second receiver having a different function, and

whereby a third key intercepted at a receiver which forms part of a first group of receivers cannot be effective to enable a receiver which forms part of a second of said group of receivers.

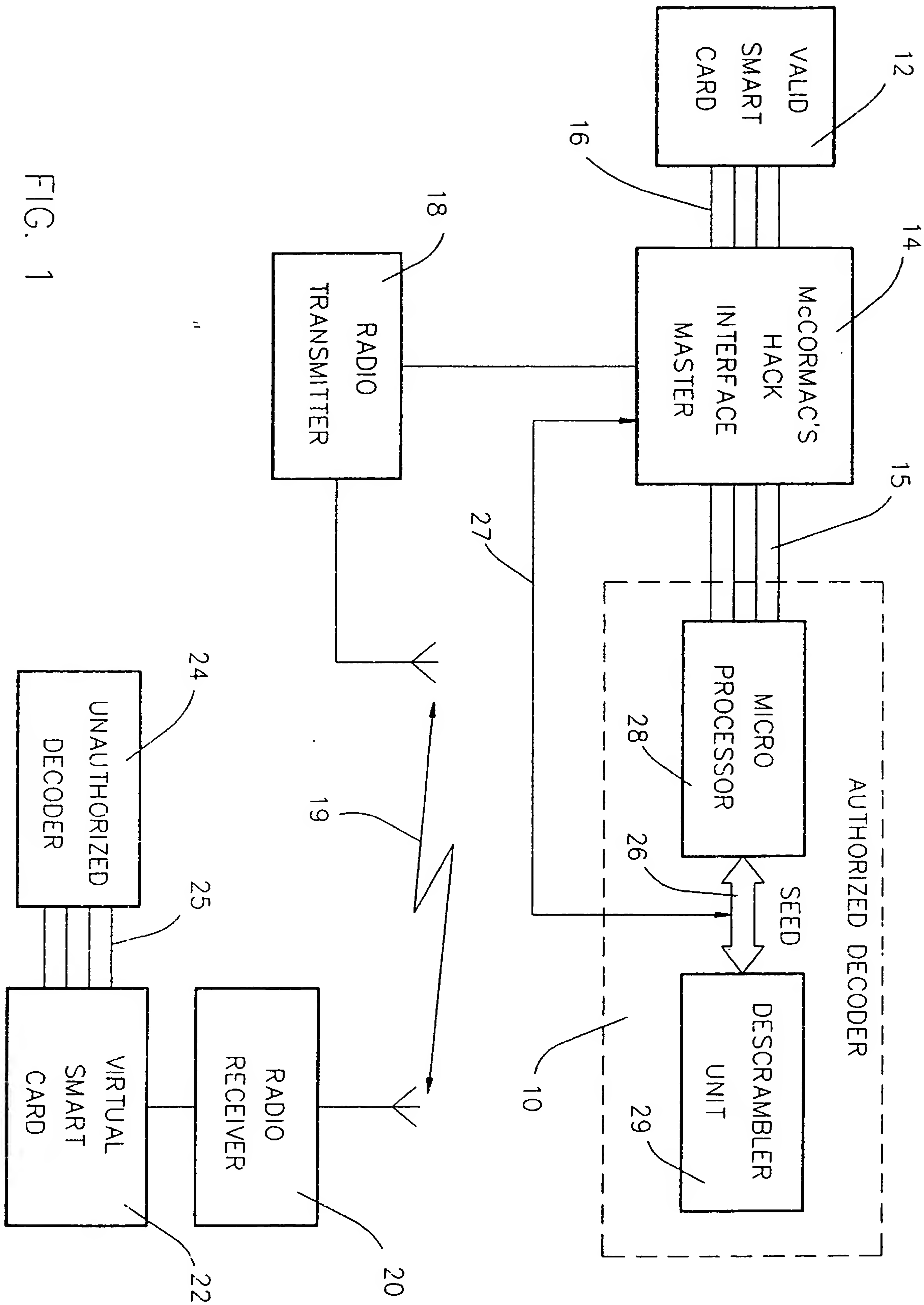
VALID SMART CARD
12
16
McCORMAC'S HACK INTERFACE MASTER
14
15
RADIO TRANSMITTER
18
27
AUTHORIZED DECODER
MICRO PROCESSOR
28
26
SEED
DESCRAMBLER UNIT
29
10
19
UNAUTHORIZED DECODER
24
25
RADIO RECEIVER
20
VIRTUAL SMART CARD
22

FIG. 1

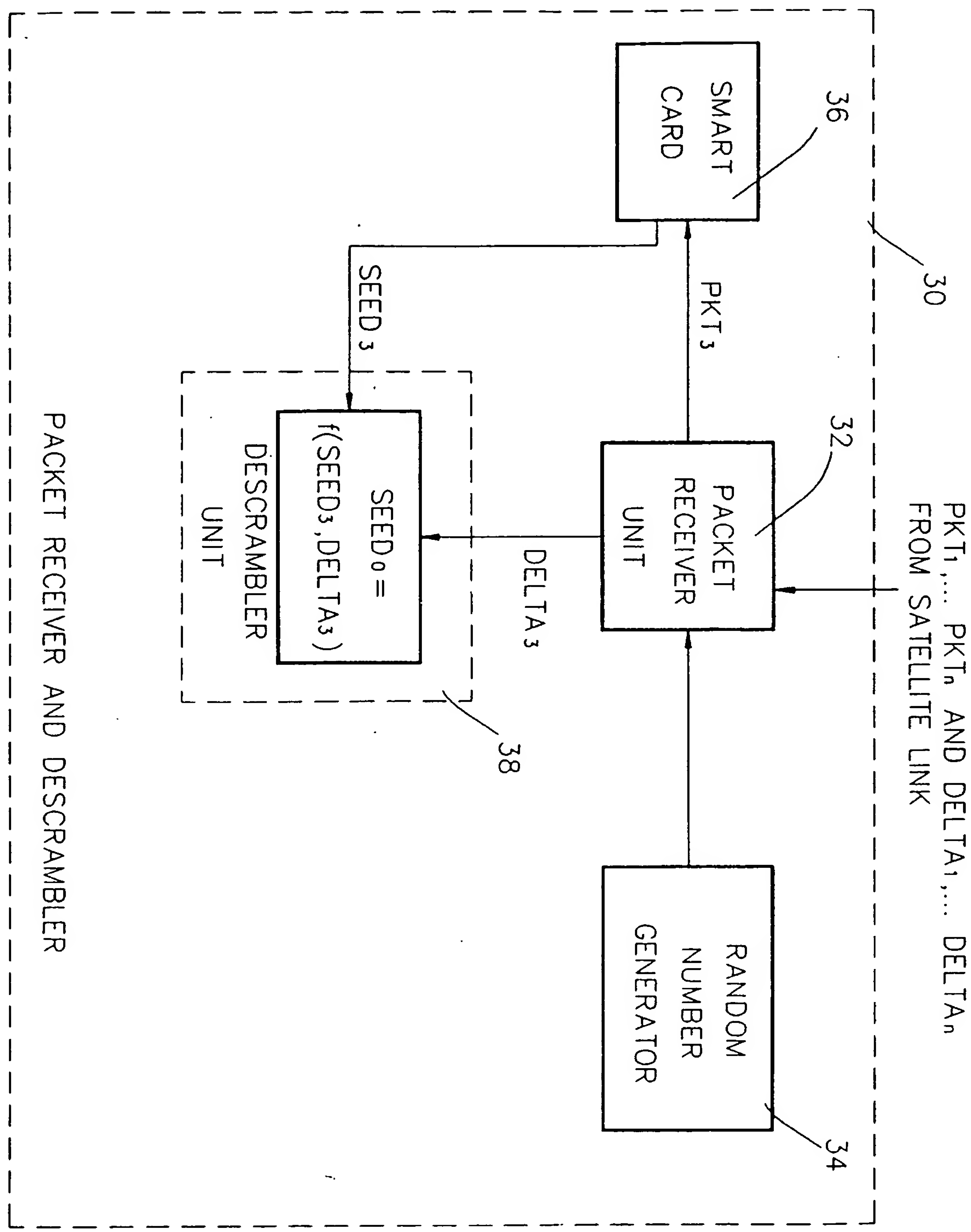
PKT1,... PKTn AND DELTA1,... DELTAn
FROM SATELLITE LINK
30
36
SMART
CARD
PKT3
32
PACKET
RECEIVER
UNIT
34
RANDOM
NUMBER
GENERATOR
SEED3
DELTA3
SEED0 =
f(SEED3,DELTA3)
DESCRAMBLER
UNIT
38
PACKET RECEIVER AND DESCRAMBLER

FIG. 2

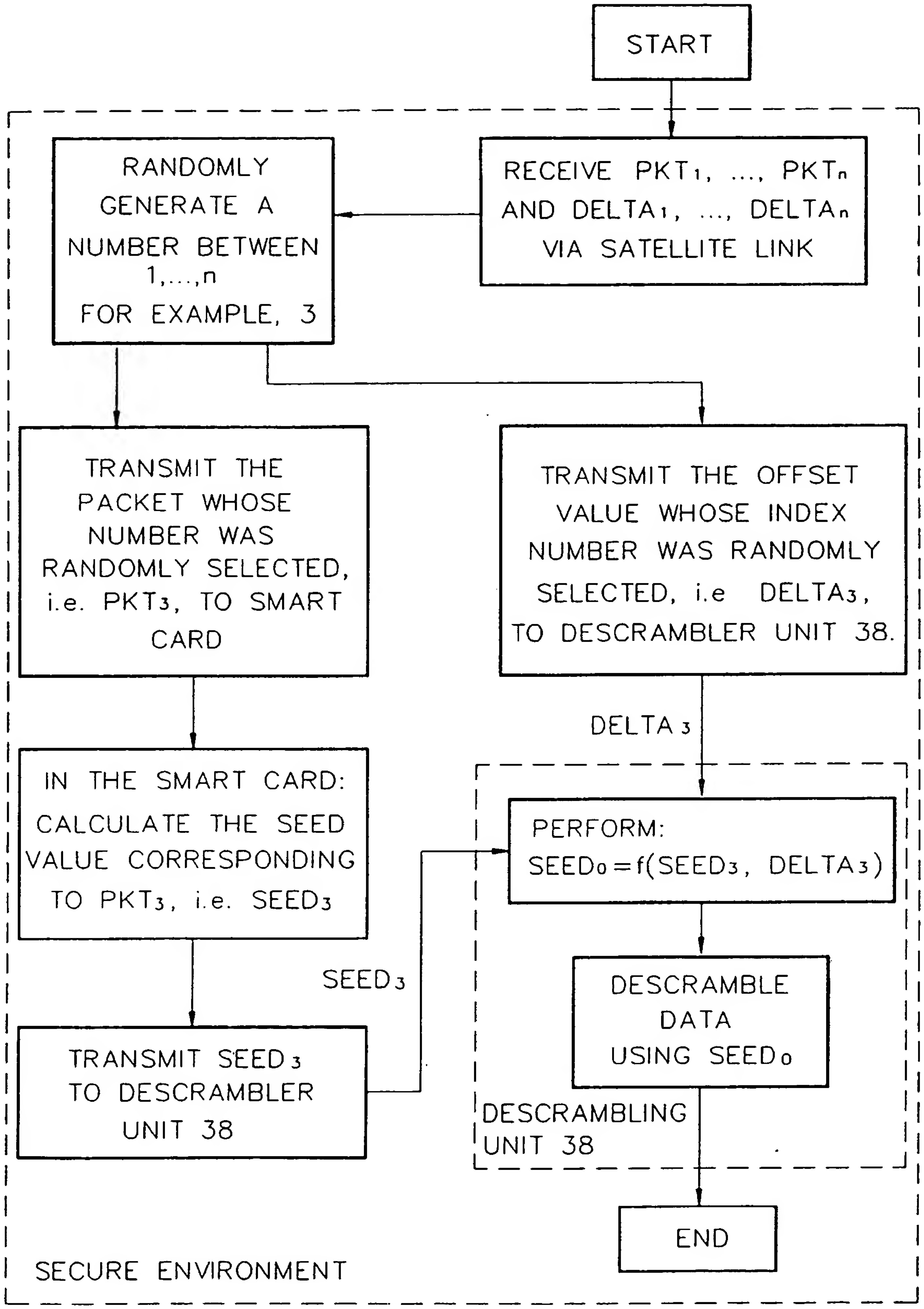
START
RECEIVE PKT1, ..., PKTn AND DELTA1, ..., DELTAn VIA SATELLITE LINK
RANDOMLY GENERATE A NUMBER BETWEEN 1,...,n FOR EXAMPLE, 3
TRANSMIT THE PACKET WHOSE NUMBER WAS RANDOMLY SELECTED, i.e. PKT3, TO SMART CARD
TRANSMIT THE OFFSET VALUE WHOSE INDEX NUMBER WAS RANDOMLY SELECTED, i.e DELTA3, TO DESCRAMBLER UNIT 38.
DELTA3
IN THE SMART CARD: CALCULATE THE SEED VALUE CORRESPONDING TO PKT3, i.e. SEED3
SEED3
PERFORM: SEED0=f(SEED3, DELTA3)
DESCRAMBLE DATA USING SEED0
TRANSMIT SEED3 TO DESCRAMBLER UNIT 38
DESCRAMBLING UNIT 38
END
SECURE ENVIRONMENT

FIG. 3

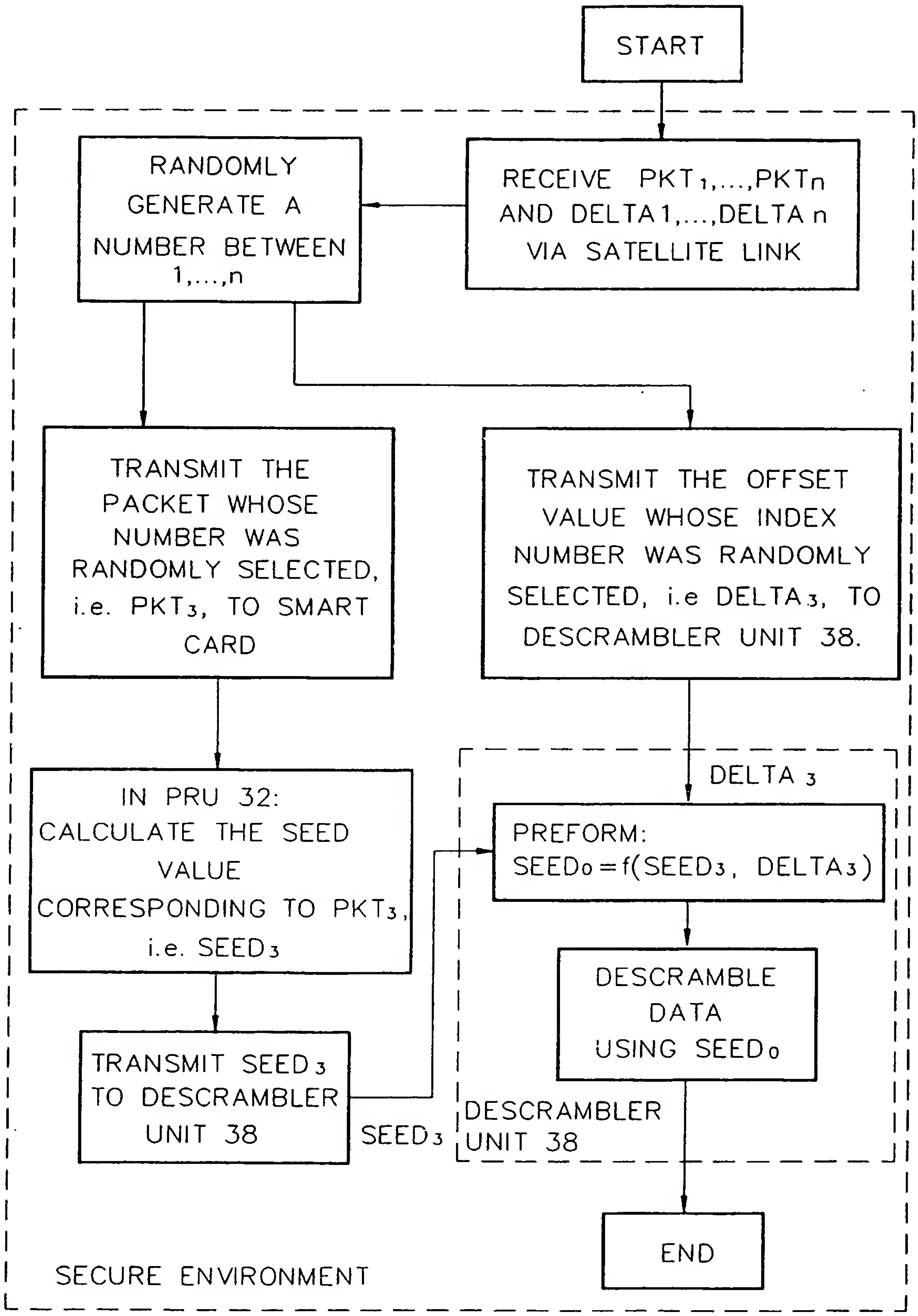
START
RECEIVE PKT1,...,PKTn AND DELTA1,...,DELTAn VIA SATELLITE LINK
RANDOMLY GENERATE A NUMBER BETWEEN 1,...,n
TRANSMIT THE PACKET WHOSE NUMBER WAS RANDOMLY SELECTED, i.e. PKT3, TO SMART CARD
TRANSMIT THE OFFSET VALUE WHOSE INDEX NUMBER WAS RANDOMLY SELECTED, i.e DELTA3, TO DESCRAMBLER UNIT 38.
DELTA 3
IN PRU 32: CALCULATE THE SEED VALUE CORRESPONDING TO PKT3, i.e. SEED3
PREFORM: SEED0=f(SEED3, DELTA3)
DESCRAMBLE DATA USING SEED0
TRANSMIT SEED3 TO DESCRAMBLER UNIT 38
SEED3
DESCRAMBLER UNIT 38
END
SECURE ENVIRONMENT

FIG. 4

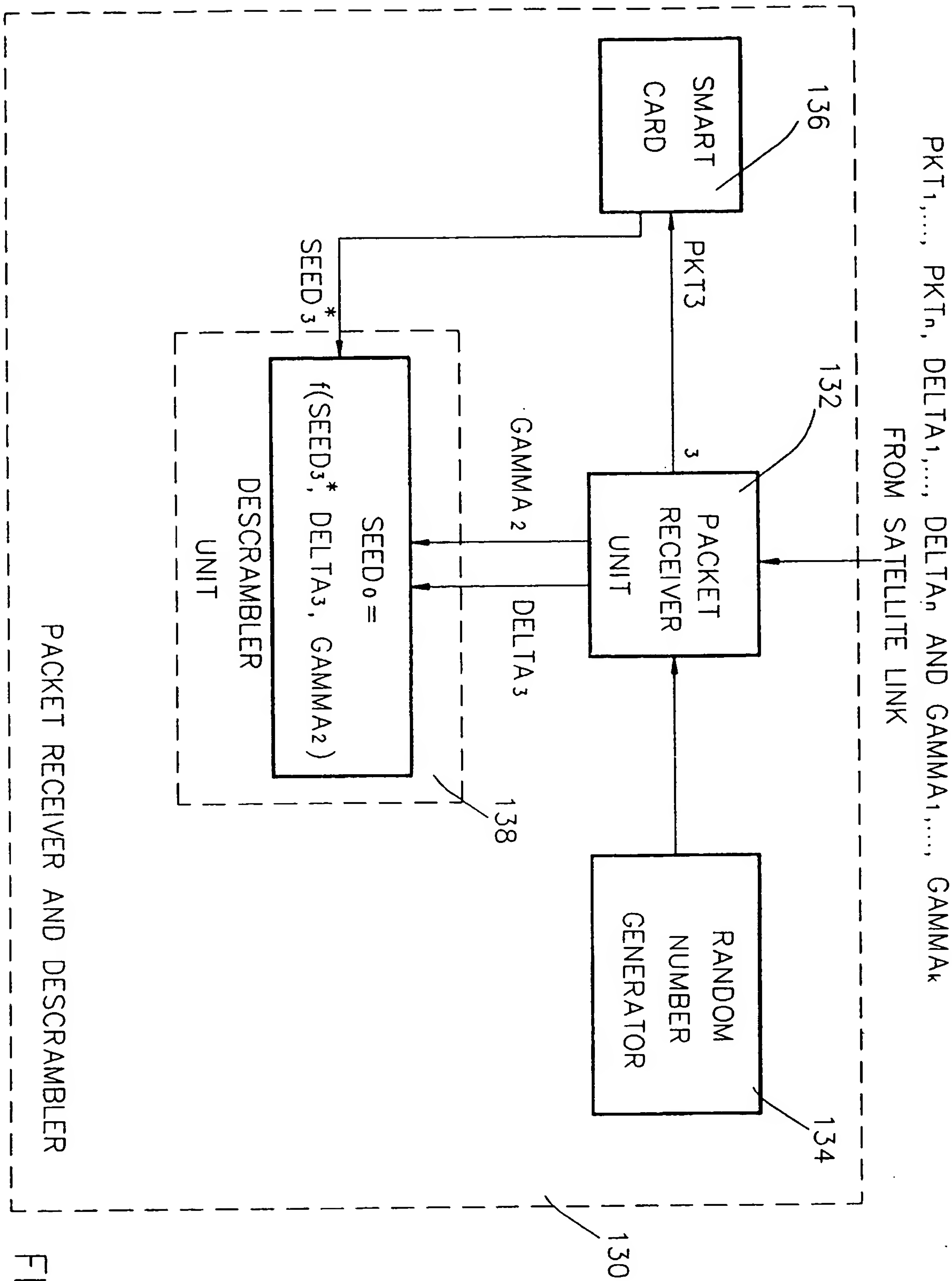
PKT1,..., PKTn, DELTA1,..., DELTAn AND GAMMA1,..., GAMMAk
FROM SATELLITE LINK
SMART CARD
136
PKT3
SEED3*
132
3
PACKET RECEIVER UNIT
GAMMA 2
DELTA 3
SEED0 =
f(SEED3*, DELTA3, GAMMA2)
DESCRAMBLER UNIT
138
RANDOM NUMBER GENERATOR
134
PACKET RECEIVER AND DESCRAMBLER
130

FIG. 5

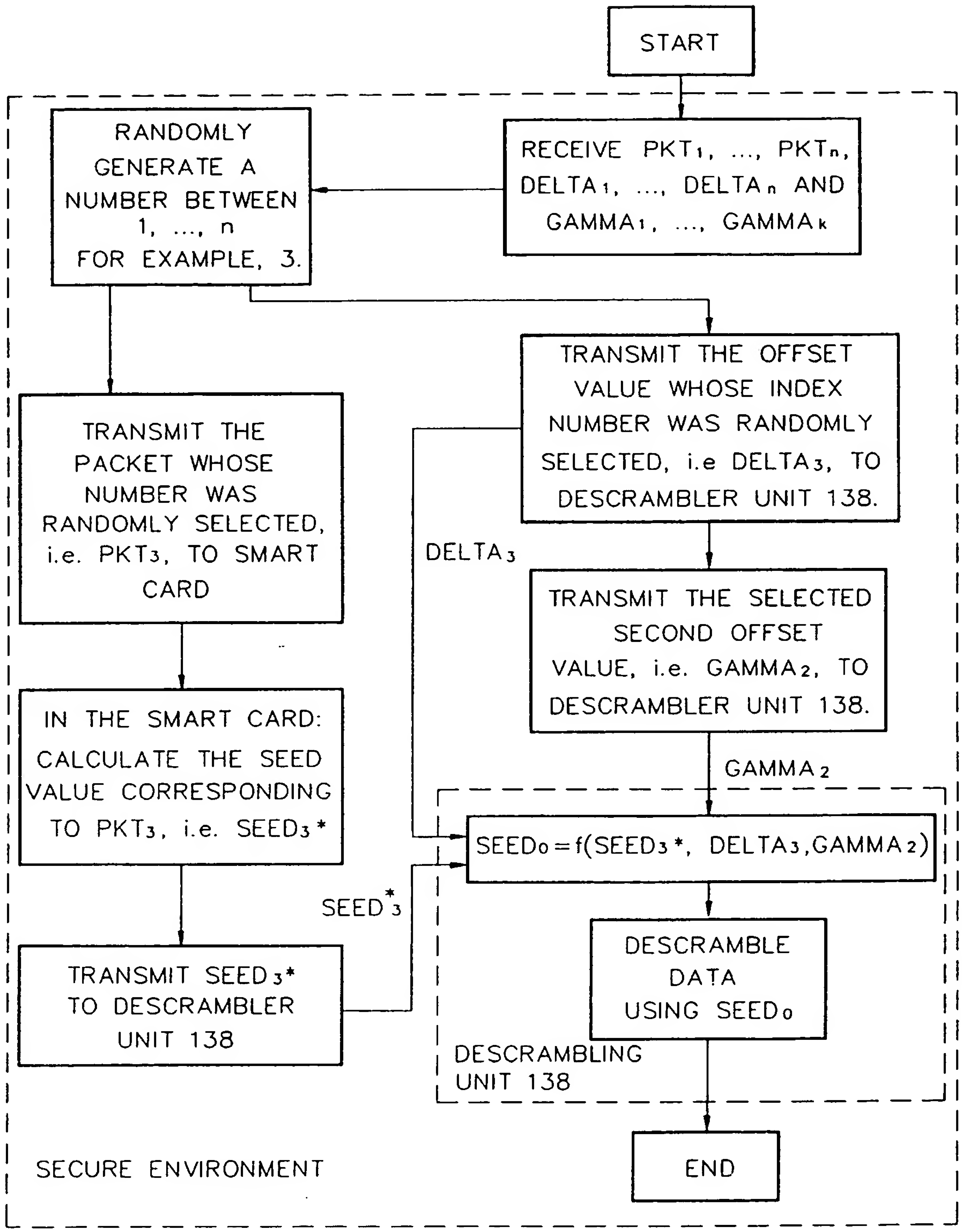
START
RECEIVE PKT1, ..., PKTn, DELTA1, ..., DELTAn AND GAMMA1, ..., GAMMAk
RANDOMLY GENERATE A NUMBER BETWEEN 1, ..., n FOR EXAMPLE, 3.
TRANSMIT THE PACKET WHOSE NUMBER WAS RANDOMLY SELECTED, i.e. PKT3, TO SMART CARD
TRANSMIT THE OFFSET VALUE WHOSE INDEX NUMBER WAS RANDOMLY SELECTED, i.e DELTA3, TO DESCRAMBLER UNIT 138.
DELTA3
TRANSMIT THE SELECTED SECOND OFFSET VALUE, i.e. GAMMA2, TO DESCRAMBLER UNIT 138.
IN THE SMART CARD: CALCULATE THE SEED VALUE CORRESPONDING TO PKT3, i.e. SEED3*
GAMMA2
SEED0=f(SEED3*, DELTA3,GAMMA2)
SEED*3
TRANSMIT SEED3* TO DESCRAMBLER UNIT 138
DESCRAMBLE DATA USING SEED0
DESCRAMBLING UNIT 138
END
SECURE ENVIRONMENT

FIG. 6